ABSTRACT OF THE DISCLOSURE

The distributed firewall performs user authentication at a first level to establish a user security context for traffic from that user, and an authority context provides authorization for subsequent traffic. This authority context may be based on an underlying policy for particular types of traffic, access to particular applications, etc. Additionally, the system includes the ability to allow a user/process/application to define its own access control. The linking of the user security context from the traffic to the application is accomplished by enabling IPSec on a socket and forcing the socket to be bound in exclusive mode. The most common policy definitions may be included by default. Extensions of the Internet key exchange protocol (IKE) to provide the desired user authentication plus application/purpose are also provided. The architecture includes pluggable authorization module(s) that are called after IKE has successfully authenticated the peer, but before the connection is allowed to complete.